DOCUMENT RESUME

ED 324 011 IR 053 286

AUTHOR Berman, Jerry; Goldman, Janlori
TITLE A Federal Right of Information Privacy: The Need for Reform. Number 4.
INSTITUTION Benton Foundation, Washington, DC.
PUB DATE 89
NOTE 43p.; Project on Communications & Information Policy Options. For related reports, see IR 053 287-288 and IR 053 300.
AVAILABLE FROM Policy Option Project, Benton Foundation, 1776 K Street, NW, Washington, DC 20006 ($6.50 per single copy, $33.00 for boxed set of eight papers).
PUB TYPE Legal/Legislative/Regulatory Materials (090) -- Viewpoints (120)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS Access to Information; Confidential Records; Constitutional Law; *Disclosure; Federal Legislation; *Information Dissemination; *Information Needs; Information Utilization; *Policy Formation; Political Issues; *Privacy; *Public Policy
IDENTIFIERS *Information Policy

ABSTRACT

Because a right of information privacy is not firmly imbedded in constitutional case law, advocates of the concept that citizens have the right to control personal information held by others turned to Congress. Enacted to regulate the government's use of personal information, the Privacy Act of 1974 has failed to work in the way intended. Shortly after its passage, the political swing away from privacy and toward bureaucratic efficiency revealed the Act's structural and conceptual weaknesses. It is suggested that this act needs to be redrafted to strengthen its major principle--i.e., that information collected for one purpose may not be used for another purpose without the individual's consent. It is also recommended that information legislation restrict access to personal information held by private institutions. Further, it is felt that public policy is needed in response to advanced information technology that imbues institutions with the power to instantly exchange, compare, verify, profile, and link information in separate databases. This report provides guiding principles for drafting legislation, and concludes that statutory standards should incorporate a balance between the sensitivity of the information at stake and the institutional justification or need for the information. (SD)

4

A Federal Right of Information Privacy: The Need for Reform

Jerry Berman & Janlori Goldman

Benton Foundation
Project on Communications &
Information Policy Options

The Benton Foundation

The Benton Foundation, based in Washington, D.C., is a private grantmaking foundation committed to improving the democratic process through increased public understanding and use of communications and information technologies. A legacy of Senator William Benton, the foundation supports projects in the fields of communications policy, public affairs and the media, and communications education.

Benton Foundation Project on Communications & Information Policy Options

In early 1988, the Benton Foundation commissioned a series of eight papers to explore future options for public policy in the communications and information arenas. Written by recognized authorities in their respective fields, the papers identify critical issues and options confronting policymakers at the federal level.

Through the publication of this series, the foundation seeks to stimulate public awareness and discussion of the communications and information issues that will affect our society in the coming decade. Two broad themes are addressed in the papers: the role of policy in the rapidly changing mass media marketplace, and the ethical, constitutional, and regulatory challenges that arise from the increasing use of computers in our society.

The views in this paper are those of the author(s), and do not necessarily represent those of the Benton Foundation, its directors, or its staff.

A Federal Right of Information Privacy: The Need for Reform

Jerry Berman & Janlori Goldman

About the Authors

Jerry Berman is the Director of the ACLU Project on Privacy and Technology and ACLU Chief Legislative Counsel. He is Co-Chair of the Privacy Committee of the American Bar Association's Section on Individual Rights and Responsibilities. Mr. Berman has worked to enact major privacy legislation including the Electronic Communications Privacy Act of 1986 and the Foreign Intelligence Surveillance Act of 1978.

Janlori Goldman is the Staff Attorney of the ACLU Project on Privacy and Technology. Ms. Goldman, formerly Legal Counsel of the Minnesota Civil Liberties Union, has participated in the development of information privacy policy. Her work has contributed to the passage of the Computer Matching and Privacy Protection Act of 1988 and the Video Privacy Protection Act of 1988.

The authors gratefully acknowledge Morton H. Halperin, Jane E. Larson, William L. Miller, and Albert Y. Muratsuchi for their invaluable assistance and support in the editing of this paper.

Executive Summary

This paper examines the right of citizens to control personal information held by others. The right of information privacy is an enduring and cherished value in this country, resonating at the heart of individual freedom, autonomy, and individuality. Crucial to one's sense of "self" is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose. Yet, individuals are increasingly losing control over personal information collected, maintained, used, and disseminated by both the federal government and private institutions.

Because a right of information privacy is not firmly embedded in constitutional case law, privacy advocates have turned to Congress. The Privacy Act of 1974, which was enacted to regulate the government's use of personal information, has failed to work in the way intended by Congress. Shortly after its passage, the political swing away from privacy and towards bureaucratic efficiency revealed the Act's structural and conceptual weaknesses. The Act needs to be rewritten to strengthen its major principle — information collected for one purpose may not be used for a different purpose without the individual's consent.

In addition, information privacy legislation is needed to restrict access to personal information held by private institutions. Congress has enacted laws to protect records held by banks, schools, the credit industry, cable and video companies, and others. These laws serve as precedents for legislation that establishes on a case-by-case basis an incremental series of privacy rights in information held by the government and private institutions, including protections for medical, insurance, personnel, and retail records. Further, public policy is needed in response to advanced information technology that gives institutions the power to instantly exchange, compare,

verify, profile, and, most importantly, link information in separate data bases.

Statutory standards should incorporate a balance between the sensitivity of the information at stake and the institutional justification or need for the information — the more sensitive the information, the more compelling the need must be for its collection, and the higher the standard must be for its disclosure to others. In this way, individuals will be able to maintain some meaningful control over personal information divulged as a condition of receiving government benefits or in the course of doing business with others.

I. INTRODUCTION

The constitutional right to privacy is, as Justice Brandeis first stated, "the right to be left alone—the most comprehensive of rights and the right most valued by civilized men."[1] Brandeis' formulation has long been the starting point for any discussion of the meaning of privacy. But what value does privacy hold for us? What does privacy look like in the late 1980s? Are we truly able, or even entitled, to live certain areas of our lives outside of the public eye? Is privacy still the most valued and comprehensive of rights?

"Who cares about privacy?"[2] National polls document a growing public demand for privacy protection. In a 1983 analysis of their survey results, Louis Harris and Associates concluded:

> Particularly striking is the pervasiveness of support for tough new ground rules governing computers and other information technology. Americans are not willing to endure abuse or misuse of information, and they overwhelmingly support action to do something about it. This support permeates all subgroups in society and represents a mandate for initiatives in public policy.[3]

Most people cherish their right to be able to live certain areas of their lives outside of the public eye.[4] Yet today, these same people are overwhelmed by institutional demands for information. Crucial to one's sense of "self" is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose. Although there is broad public support for privacy, individual voices are often scattered and powerless, forcing a reliance on organized constituencies.

The confirmation hearings of Judge Robert Bork to the United States Supreme Court brought home the degree to which an individual's sense of freedom and identity depends on governmental respect for privacy. Voicing this belief, the majority of Senators who voted against Judge Bork's confirmation expressed concern over Bork's hostile view of the constitutional right to privacy.

Citizens are losing control of personal, sensitive information as government agencies and private institutions escalate the collection and exchange of personal information. In 1988, a number of federal agencies proposed massive expansions of their information systems by linking their records with the separately maintained record systems of other agencies. The FBI, for example, proposed enhancing its law enforcement efforts by connecting its National Crime Information Center (NCIC) to the computerized record systems of the Department of Health and Human Services (HHS), the Internal Revenue Service (IRS), the Social Security Administration (SSA), and the Immigration and Naturalization Service (INS). The Bureau's plan was ultimately defeated, in part due to the efforts of privacy advocates and computer security experts who submitted a report to the agency recommending that the linkage proposal be abandoned.[5] However, other proposals may soon be implemented. HHS recently announced its plan to link electronically thousands of computers containing the prescription records of Medicare beneficiaries in pharmacies nationwide. HHS claims this new system will streamline the Medicare bureaucracy.[6]

Many have long feared that such coordinated information collection would eventually lead to the creation of a national database containing lifetime dossiers on all citizens, held in one centrally controlled mainframe computer. However, advanced information technology now allows information maintained in completely separate databases to be linked. In a recent study, the Office of Technology Assessment (OTA) concluded that a *de facto* national database already exists on U.S. citizens.[7] Privacy legislation is necessary to respond to the present reality that advanced information technology now gives institutions, both public and private, the power to nearly instantly exchange, compare, verify, profile, and most importantly, link information.

Technology has overtaken current law, leaving society without a new set of social mores to limit and define the extent to which advanced technology can be used to know all we can about each other. The danger is that a watched society is a conformist society, one in which people are afraid to act or believe in ways that call

attention to themselves or arouse suspicions. As one commentator observed:

> [A person] who is compelled to live every minute of . . . life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of . . . individuality and human dignity. Such an individual merges with the mass. [That person's] opinions, being public, tend never to be different; . . . aspirations, being known, tend always to be conventionally accepted ones; . . . feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every [person]. Such a being, although sentient, is fungible, [and] is not an individual.[8]

This paper addresses a number of different information privacy[9] issues and examines the reasons why information privacy is an enduring and cherished value in this country, resonating at the heart of individual freedom, autonomy, and individuality. The right of individuals to control information about themselves once they have given it over to a governmental entity is examined. The Privacy Act of 1974 — the federal law regulating the government's collection, dissemination, maintenance, and use of personal information — is discussed in depth, including an analysis of its legislative history, implementation, and shortcomings. The right of individuals to control information about themselves once they have given it over to a private institution is also examined. In this context, the paper considers whether there is a constitutional basis for information privacy. In conclusion, the paper recommends a proposed rewrite of the Privacy Act and a policy blueprint for future information privacy initiatives to protect records held by the private sector.

II. IS THERE A CONSTITUTIONAL BASIS FOR A RIGHT OF INFORMATION PRIVACY?

Although the right to privacy is not explicitly granted by the U.S. Constitution, the United States Supreme Court has interpreted

the Constitution to grant individuals a right of privacy, based on the First Amendment freedom of association and expression,[10] the Fifth Amendment privilege against self-incrimination,[11] penumbras of the Bill of Rights and the Ninth Amendment,[12] the Fourteenth Amendment's guarantee of "ordered liberty",[13] but principally rooted in the Fourth Amendment protection of persons, places, papers, and effects against unreasonable searches and seizures.[14] The primary concern of this section is whether there is a constitutional right to privacy in personal information held by others and whether restrictions may be placed on personal information held by the government.

The Fourth Amendment was drafted two hundred years ago to curtail the "writs of assistance" used by officials to search door-to-door for British tariff law violations. The Framers could not imagine today's widespread collection and use of personal information by businesses and other institutions or the massive and easily accessed body of personal information held by the government. In the 1700s, "personal information was difficult to collect, and files were handwritten, rarely reproduced and easily lost."[15] However, despite major changes in the way individuals handle their papers, the Court has been reluctant to extend the reach of the Fourth Amendment to protect records from intrusion once they are held by someone else.

The application of the Fourth Amendment had traditionally hinged on property-based notions of liberty that ground peoples' rights in their relationships to particular places, such as the "home-as-castle." However, in an early case, *Boyd v. United States*, the Supreme Court brought the Fourth Amendment into the late nineteenth century, reasoning that the founding principles of the Amendment were broadly worded to

> apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of his life. It is not the breaking of his doors or the rummaging of his drawers that constitute the essence of the offense, but it is the invasion of his indefensible right of personal security, personal liberty and private property.[16]

The Fourth Amendment, the *Boyd* Court noted, reflects the colonists' struggle with the arbitrary power of government. Thus, they cautioned, "constitutional provisions for the security of property and person should be liberally construed. A close and literal construction deprives them of half of their efficacy, and leads to a gradual depreciation of the right, as if it consisted more in sound than in substance."[17] The Justices recognized that the Fourth Amendment protection of property extends to government intrusions outside one's home.

The Constitution also has been interpreted to extend protection to information that implicates both First Amendment and privacy values. In *NAACP* v. *Alabama*,[18] the Court recognized the severe chilling effect on First Amendment freedoms that can result from the unauthorized disclosure of an organization's membership, finding damage in the mere revelation of one's personal, political beliefs.

In 1967, the Supreme Court, in ruling that warrantless wiretapping is unconstitutional, held that the Fourth Amendment protects people, not places. (*Katz* v. *United States*.[19]) In *Katz*, the Court set forth a standard for determining constitutionally protected "zones of privacy" — whether the expectation of privacy in the area to be searched outweighs the government's interest in searching that area, factoring into this analysis the degree of intrusion involved. With *Katz* and preceding cases, the Court developed an interpretation of the Fourth Amendment, and the Bill of Rights as a whole, as protections not only of tangible property, but also of an individual's communications, personality, politics, and thoughts.

The problem with the *Katz* formulation is that its relative standard — a "reasonable expectation of privacy" — can only reflect, not prevent, deterioration in societal respect for privacy. Applying this "reasonable expectation" standard, the Court in later cases often determined that an individual's privacy had not been violated by certain intrusions because society's "expectation of privacy" had been persistently lowered by the circumstances of modern existence. Many people can no longer claim to reasonably expect privacy even in the most intimate activities of their lives.[20]

In a recent case, for example, the Court ruled that the Fourth Amendment protection against unreasonable searches and seizures does not extend to one's garbage once it is removed from the home. The Court rationalized that the garbage is placed on the curb "for the express purpose of conveying it to a third person." (*California* v. *Greenwood*.[21]) The Court did not place great emphasis on the fact that the garbage owner intended to convey the garbage to the trash collector and not to the police. In this context, it is nearly impossible for one to reasonably tie one's intentions to one's expectations. As one commentator has argued, the flaw in the Court's reasoning in *Greenwood*:

> is that constitutionally protected security is not lost merely because some invasion may be expected from some invader. The Fourth Amendment protects a car parked overnight on a city street although the owner knows that thieves frequently break into parked cars to steal radios. . . . So it cannot be, as the majority would have it, that a citizen's security is totally lost by the reasonable anticipation that someone — illegally, officially or casually — is likely to penetrate an otherwise protected space. We commonly relinquish interest and control to limited classes of people and for limited and specific purposes.[22]

One's constitutional rights should not depend on the extent to which institutions wear down societal expectations of privacy. Nowhere is the fallibility of the *Katz* "reasonable expectation of privacy" standard more evident than in the Court's holding in *United States* v. *Miller*.[23] The Court in *Miller* ruled that one does not have a constitutionally protected privacy interest in personal records held by a bank. The Court found that a person's bank records do not fall within the "zone of privacy" and are not therefore within the scope of the Fourth Amendment. Bank records may thus be made available to law enforcement without a showing of probable cause to believe that a crime has been committed. The *Miller* decision ultimately turned on the fact that the bank customer could not assert ownership of his documents. The Court held that because Miller's documents were the bank's business records, the expectation of

privacy he asserted was not reasonable.[24] The Court reached this conclusion even though most bank customers probably do have an expectation of privacy in these records.

The Court in *Miller* applied a flawed principle. Banks maintain customer records both as a service to customers and for the banks' own recordkeeping purposes. The customer may voluntarily relinquish physical possession of his or her records (or maintain duplicates) but clearly does not intend to lose all control over those records.[25] Customers continue to maintain an interest in the records of a transaction because those records directly represent the transaction. As Justice Brennan dissented in the 5-4 opinion in the *Miller* case:

> A bank customer's reasonable expectation is that, absent a compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. . . . [A] depositor reveals many aspects of his personal affairs, opinions, habits, associations. Indeed, the totality of bank records provides a virtual current biography. . . . Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[26]

People do expect that they are entitled to privacy in their financial affairs. Such a right is essential in a modern society. Financial records, and other records that reflect what we buy, where we travel, what we read, who we communicate with, are extensions of our selves, regardless of where they are stored. They are the "papers" explicitly and separately named as protected by the Fourth Amendment. Nowhere in the Amendment does it say that one's papers must be kept in the home in order to be safe from unwarranted government intrusion.

The *Miller* decision demonstrates the Court's unwillingness to bring the Fourth Amendment into the information age. The fundamental principle of the Fourth Amendment — that individuals have the right to be secure against unreasonable searches and seizures by the government — requires the government to justify the privacy intrusions that result from these searches. However, the Court in *Miller* refused to make the conceptual leap to apply this constitutional standard to personal information held by others.

If there is a constitutional basis for privacy in records stored in the home, the Bill of Rights must also recognize information as private when stored or maintained outside the home. Refusing, however, to move beyond the era in which people stored their personal papers and records in the home, the Supreme Court has stopped short of extending constitutional protection to personal information held by others from whom we receive services and with whom we do business. Although modern society may change the form in which information is stored, the conflict between the government's interest in expanding its power through access to personal information, and the individual's interest in retaining a sphere of autonomy against that power, remains the same.

If, as the Supreme Court stated in *Katz*, the Fourth Amendment protects people and not places, it follows that the price of engaging in often unavoidable transactions should not be that we are forced to relinquish any expectation that transactions outside the home are private, particularly given the highly sensitive and intimate nature of many records. Financial, and most other, records generated in the course of one's life, reveal an enormous amount about an individual. More importantly, the combination of separately maintained personal records enables both the prosecutor and the merely curious to create a lifetime dossier and an individual biography.

The Court has only rarely dealt with the issue of whether there are constitutional limits to the government's ability to use personal information that it lawfully possesses. Shortly after the *Miller* decision in 1977, the Supreme Court ruled in another information privacy case on whether the government's mere collection and

maintenance of personal information in centralized, computerized files rises to the level of constitutional invasion into an individual's privacy. In *Whalen* v. *Roe*,[27] the Court held that a state may maintain files containing the names and addresses of all people who lawfully obtain prescription drugs. The Court found that although one may assert a constitutional privacy right to not disclose personal matters, the state's centralized file did not pose a "sufficiently grievous threat to disclosure." In one sense, *Whalen* may be viewed as a positive decision because the Court upheld the statute in question on the grounds that it incorporated "due process safeguards," such as confidentiality and security provisions, to protect against unwarranted disclosures.

The *Whalen* Court asked whether the government's collection of personal information posed a threat to privacy, and decided that it did:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. [We] recognize that in some instances that duty arguably has its roots in the Constitution. . . . Broad dissemination of such information, however, would clearly implicate constitutionally protected rights. . . .[T]he central computer storage of the data thus collected. . . vastly increases the potential for abuse of that information.[28]

The Fourth Amendment is elastic enough to apply to privacy intrusions created by advances in information technology and policy. Because the Court has rigidly refused to expand the scope of the Fourth Amendment to explicitly recognize the right to be secure in one's personal papers held by others, privacy advocates have turned to Congress to address the issue in legislation. Congress has responded by creating zones of privacy around certain information, and enacting a number of information privacy statutes in direct response to Supreme Court decisions.[29]

III. THE CONGRESSIONAL RESPONSE

A. The Privacy Act of 1974

Congress has struggled with the problems posed by increasing information collection and use, and the development of new information technologies that transform the way institutions handle information. In the 1960s and early 1970s, Congress held a series of hearings on computers, privacy, and the protection of personal information.[30] Throughout most of the 1960s, Congress considered a proposal to create a centralized national data center on all U.S. citizens containing information such as Social Security numbers, and income and census data. Backers of the proposal argued that the center was necessary to serve the needs of the "welfare state." After years of hearings, studies, and debates, the national data center was overwhelmingly condemned as "Big Brother" government, and a threat to individual autonomy, dignity, and liberty.

At a 1966 hearing, one Representative expressed fear that a centralized federal facility, into which would be "poured information collected from various government agencies and from which computers could draw selected facts, . . . could lead to the creation of . . . the 'Computerized Man'. . . stripped of his individuality and privacy."[31] At the same hearing, Representative Frank Horton (R-NY) extolled the virtues of inefficiency and bureaucracy: "One of the most practical of our present safeguards of privacy is the fragmented

nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard."[32] The plan was abandoned.[33]

It should be noted that one witness at the 1966 hearing on "The Computer and the Invasion of Privacy" warned privacy advocates of the dangers of focusing attention on the central data bank issue:

> The problems of the invasion of privacy are, in my view, significant, and they will exist whether or not the central computer bank is created by the Government. Individual data systems, both public and private, now being developed, can be tied together eventually into a network that will present essentially the same problems.... Today we are already building the bits and pieces of separate automated information systems in both the private and government sectors that so closely follow the pattern of development to the present integrated communications structure that a de facto version of the system you are now pondering is already in the construction phase. It is in many ways more dangerous than the single data bank now being considered.[34]

By 1973, the Watergate scandal contributed to what had become a national crisis of faith in government institutions and a heightened sensitivity to the unfettered ability of the government to intrude into the personal affairs of its citizens. In this environment, the public became increasingly concerned about the unhampered collection and use of personal records by the government:

> Accelerated data sharing of such personally identifiable information among increasing numbers of federal agencies through sophisticated automated systems, coupled with the recent disclosures of serious abuses of governmental authority represented by the collection of personal dossiers, illegal wiretapping, surveillance of innocent citizens, misuse of tax data, and similar types of abuses, have helped

to create a growing distrust or even fear of their government in the minds of millions of Americans.[35]

In 1973, an advisory committee within the Department of Health, Education, and Welfare (HEW) published a report entitled *Records, Computers and the Rights of Citizens*,[36] proposing a Code of Fair Information Practices to be used by federal agencies. The basic principles of the Code, which was incorporated into the Privacy Act of 1974 and became legally binding on agencies, are: 1) there must be no personal data record-keeping systems whose very existence is secret; 2) there must be a way for an individual to find out what information is in his or her file and how the information is being used; 3) there must be a way for an individual to correct information in his or her records; 4) any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and 5) there must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without consent. This last principle became the heart of the Privacy Act and the information privacy legislation that followed. In passing the Privacy Act of 1974, Congress explicitly recognized that:

1) The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

2) The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

3) The opportunities for an individual to secure employment, insurance, and credit and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

4) The right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

5) In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.[37]

In introducing the Senate version of the Bill, Senator Sam Ervin (D-NC) said: "[T]he appetite of government and private organizations for information about individuals threatens to usurp the right to privacy which I have long felt to be among the most basic of our civil liberties as a free people. . . . [T]here must be limits upon what the government can know about each of its citizens."[38] In drafting the Privacy Act, Congress sought to block the creation of a national data center containing personal information, and curtail the use of the Social Security number (SSN) as a uniform national identifier. Further, Congress found that '[i]f the use of the SSN as an identifier continues to expand, the incentives to link records and broaden access to them are likely to increase."[39]

The purpose of the Act was to "promote accountability, responsibility, legislative oversight and open government with respect to the use of computer technology in the personal information systems and databanks of the federal government."[40] The Act was to serve as an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" for federal agencies.

To accomplish these goals, the Act establishes a right of privacy in personal information held by federal agencies. With certain exceptions, the Act prohibits government agencies from disclosing information collected for one purpose for a different purpose without the individual's consent. Under the Act, citizens have a right of access to their records and the opportunity to amend their records upon showing that they are not accurate, relevant, timely, or complete. The Act also limits the use of the Social Security number for identification purposes, unless otherwise authorized by law, and

prohibits the government from collecting information on the political activities of citizens. Individuals may sue for injunctive relief to enforce some of the Act's provisions, and damages may be awarded by proving that harm occurred as the result of a willful or intentional agency violation of privacy.

The Privacy Act reflects a compromise between very different House and Senate passed bills. The Senate bill created a Privacy Board with oversight powers. The House bill, supported by the Ford Administration, emphasized access to and correction of records. In the final negotiations, many of the stronger Senate provisions were dropped.

Despite the good intentions and clear objectives of its drafters, the Privacy Act has fallen far short of achieving many of its original goals, at best serving as a procedural hoop-jump for federal agencies. A number of factors have severely undermined the Act's effectiveness, including flaws in the Act itself, administrative interpretation, and lack of enforcement. The basic principles of the Privacy Act have failed to limit significantly the government's use of personal information. In fact, agencies have escalated the collection and dissemination of personal information.[41]

For instance, Congress' original intent in enacting the Privacy Act was thwarted by the government's interpretation of the "routine use" exemption, which allows agencies to disclose personal information if the disclosure is *compatible* with the purpose for which it was collected.[42] Government officials have interpreted the exemption to allow the computerized matching of separate agency record systems, arguing that detecting waste, fraud, and abuse in government programs is a legitimate government interest, and is thus compatible with <u>any</u> original purpose for which records were collected.[43]

The legislative history of the Act, though, makes it clear that the routine use exemption was intended to facilitate the exchange of information for "*housekeeping measures*," such as completing payroll checks. The purpose of the exemption was to "discourage the

unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material."[44] A witness at a recent congressional hearing on computer matching testified that the "routine use provision is so big an exemption that you could drive a truck through it."[45]

The government's sweeping interpretation of the exemption contradicts the Act's core provision — that, as a general matter, information collected for one purpose may not be used for a different purpose without the individual's consent.

Debate over the Act's routine use exemption began in 1977 when the Carter Administration instituted "Project Match," a scheme to use computers to compare the Department of Health, Education, and Welfare's (HEW) list of welfare recipients with the Civil Service Commission and the Defense Department federal payroll files in eighteen states. This proposed matching of computerized lists sparked a heated feud between those who viewed matching as an important investigative and auditing tool, and those who believed that the matching of records violated the Privacy Act and intruded on individual liberties.

Many agency officials cited the Act's routine use exemption to justify extensive, inter-agency matching. However, a literal reading of the exemption does not appear to permit matching. In a 1977 letter to HEW, the Civil Service Commission's General Counsel opposed "Project Match" on the grounds that the matching of disparate records violated the Privacy Act. He argued: "Although the literal terms of [the exemption] obviously can not be followed with precision in practical application to agency operations, it is evident that this information on employees was not collected with a view toward detecting welfare abuses."[46] The Commission's counsel went further:

> At the matching stage there is no indication whatsoever that a violation or potential violation of law has occurred... It cannot fairly be said . . . that disclosure of information

about a particular individual at this preliminary stage is justified by any degree of probability that a violation or potential violation of law has occurred.[47]

The computer matching proponents prevailed. "Project Match" went forward and touched off widespread computer matching within the federal government.[48] The outcome of this debate marked the political swing away from privacy and towards bureaucratic efficiency and revealed the Privacy Act's structural and conceptual weaknesses.

The Privacy Act also prohibits a local, state, or federal agency from requiring an individual's Social Security number as a condition of receiving services or benefits, unless this is authorized by law.[49] The drafters were concerned that the Social Security number was on its way to becoming a national identifier, and would be used as the uniform identifier in linking separate records systems. Yet, Congress has since not only authorized the use of the number, but mandated it. The most striking example is the 1986 Tax Reform Act provision requiring all children over the age of five claimed as dependents on tax returns to have a Social Security number.[50]

To make matters worse, it is extremely difficult for individuals harmed by violations of the Act to bring suit under the Act. The Act's lack of both a broad injunctive relief and liquidated damages provision prevent meaningful litigation of the Act's intent and application. Privacy violations often result in intangible harm to individuals, making it very difficult to prove actual damages as required by the Act.[51]

In 1977, at the height of the initial controversy over the legality of computer matching, the Privacy Protection Study Commission, charged with studying the issues raised by the Privacy Act and recommending future legislation, issued its report: *Personal Privacy in an Information Age*.[52] The Commission was created by the Privacy Act in a provision adopted during final negotiations and accepted as less controversial than creating an Executive branch oversight agency.

The Commission's report recommended that the Privacy Act be more vigorously enforced, and suggested a number of ways to make the Act more effective. The Act, the Commission found, "has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect."[53] The report included a proposed revision of the Act that clarified ambiguities, provided individuals with broader remedies, and tightened the "routine use" exemption. The Commission found that the exemption had "unintended effects," and had been "applied loosely and exclusively from the agency's point of view."[54] It is important to note that these recommendations were published *prior to* the entrenched institutionalization of computer matching. The Commission also recommended that Congress pass additional information privacy legislation to protect information held in private sector databases.

Some privacy advocates blame the Act's failure on Congress' failure to create a federal privacy oversight agency to implement the law. The drafters of the Act did delegate oversight and guidance responsibilities to the Office of Management and Budget (OMB). However, the Privacy Commission, in its report, found that "neither OMB nor any of the other agencies. . . have played an aggressive role in making sure that the agencies are equipped to comply with the Act and are, in fact, doing so. . . . [M]uch of the early momentum appears to have been lost."[55] By 1983, the general consensus among privacy advocates was that OMB had "virtually abdicated responsibility"[56] for enforcing and overseeing the Act.

The Privacy Act is now viewed as a law that requires agencies merely to *notify* individuals before using personal records for a purpose different from that for which they were collected. Notice has become synonymous with consent. Under the Act, individual control over personal information is illusory. As Representative Glenn English (D-OK) remarked during 1983 Privacy Act oversight hearings:

> One of my chief concerns is that the bureaucracy, with the approval of OMB, has drained much of the substance out of

the Act. As a result, the Privacy Act tends to be viewed as strictly a procedural statute. For example, agencies feel free to disclose personal information to anyone as long as the proper notices have been published in the Federal Register. No one seems to consider any more whether the Privacy Act prohibits a particular use of information.[57]

The Act's core principles gave way under pressure from the "rise of the computer state,"[58] which provided the government with a hard-to-resist temptation to shift its emphasis away from giving individuals some control over personal information to fostering a system of nearly unrestrained collection and use. The political pendulum swung away from protecting privacy and fostering government accountability and towards improving bureaucratic efficiency. Today, the official presumption appears to be the more the government knows about you, the better.

A recent development in government efficiency is the use of a technique called "front-end verification." This technique allows government officials to verify information electronically by matching records on a case-by-case basis *at the time* an individual applies for benefits; i.e., at the "front end." For bureaucrats, the appeal of front-end verification is that it reduces benefit payment errors; noneligibility is detected before, rather than after, an individual has received any benefits. Some argue that this process is less of a privacy intrusion than traditional matching because it involves a search through a particular person's files rather than a massive search or "fishing expedition." However, the unchecked growth of verification systems linking various databases of personal information on every citizen poses a serious danger to individual autonomy and privacy.

The success of front-end verification depends on systems that provide rapid access to complete and accurate information. The threat is thus the same as in computer matching — concern for efficiency presses for the aggregation and linkage of multiple agency data bases to create a *de facto* national data base on all citizens. In fact, an FBI Advisory Policy Board recently proposed providing the

Bureau access to the record systems of the Department of Health and Human Services, the Internal Revenue Service, the Social Security Administration, and the Immigration and Naturalization Service. For now, the Bureau's attempt to create a federal agency clearinghouse of information for use by the law enforcement community has been defeated.[59]

Despite the long-standing concerns of Congress and privacy advocates about the government's attempt to establish a national data center, it appears that a *de facto* national data base already exists, sustained by on-line linkages that allow information to be stored in decentralized form, but instantly assembled at the press of a button. A crucial element in this data base linkage is the use of one form of identification, most often the Social Security number.

Congress has encouraged this development by enacting legislation that undermines the Privacy Act's original principles, allowing greater information collection and exchange through the mandated linkage and comparison of personal information held in separate data bases, and requiring the use of the Social Security number to facilitate this process. For instance, in establishing the Income Eligibility Verification System (IEVS) in the Deficit Reduction Act of 1984, Congress authorized the use of the Social Security number for all needs-based programs to make possible the accurate identification of applicants and to permit the computerized retrieval of information on applicants in discrete data bases containing information on wage, pension, unemployment insurance, and other income data, including unearned income from Internal Revenue Service (IRS) files.[60]

In addition, the Tax Reform Act of 1986 includes a provision requiring all children over the age of five who are claimed as dependents on a tax return to have a Social Security number.[61] The stated reason for this sweeping requirement is to catch non-custodial parents who claim their children as dependents. Although tax fraud is a legitimate government problem, this provision reflects Congress' current unwillingness to address the threat posed by a national identification system that numbers all individuals for government record-keeping purposes.[62]

Front-end verification — and the systems needed to sustain it-- pose the grave problem of greater collection of and access to personal information, resulting in the ultimate loss of individual control, autonomy, and dignity. It is not only the danger of being "just a number" that is of concern here, but also providing the government and private institutions the ability to track and profile us from birth to death, creating what Arthur Miller termed a "womb-to-tomb dossier."[63]

Despite its apparent abandonment of privacy as a primary goal of federal policy, in 1988 Congress enacted the first significant amendment to the Privacy Act. The Computer Matching and Privacy Protection Act of 1988[64] brings the computerized matching of records under the wing of the Act. Under the new law, matching is no longer treated as a "routine use" of personal records held by federal agencies The Act prohibits agencies from taking any adverse action against an individual based on a match until the results have been independently verified. Before conducting a match, agencies must now enter into written agreements specifying the purpose of the match, the records to be matched, and a cost/benefit analysis of the match The legislation does not limit in any way the content or types of records that can be matched, but does create an important procedural framework of more adequate notice to individuals, the right to a hearing before benefits are cut off or denied, and mandatory reporting requirements for agencies that match records.

B. Protecting Personal Records Held By Private Institutions

In the last eighteen years, Congress has made substantial progress in legislation regulating government and private access to privately held personal information.

— In 1970, Congress passed the Fair Credit Reporting Act,[65] prohibiting credit and investigation reporting agencies that collect, store, and sell information on consumers' credit worthiness from disclosing records to anyone other than authorized customers. The

Act requires the agencies to allow consumers to review their own records and correct inaccurate information. The legislation created a legal framework in which the reporting companies could operate, and was passed in response to the public's growing awareness and concern about personal information maintained by credit reporting bureaus.

— Four years later, the Family Educational Rights and Privacy Act[66] was passed, limiting disclosure of educational records to third parties. The law requires schools and colleges to let students see their records and challenge and correct inaccurate information in their records.

— In 1978, Congress passed the Right to Financial Privacy Act,[67] in response to the Supreme Court's decision on the privacy of bank records in the *Miller* case and in direct response to the Privacy Protection Study Commission's recommendation that *Miller* be superceded by remedial legislation. Congress strengthened the Privacy Act's "consent" principle by creating a statutory Fourth Amendment protection for bank records. The Right to Financial Privacy Act includes a minimum due process standard, and a court order provision that requires law enforcement to meet a standard of relevance before records can be released. The Act is the result of a hard-won compromise between the civil liberties community, bankers, the Department of Justice, and Congress.

— In 1980, Congress passed the Privacy Protection Act[68] to prohibit the government from searching press offices without a warrant if no one in the office is suspected of committing a crime.

— In 1982, Congress passed the Debt Collection Act[69] requiring federal agencies to provide individuals with due process protections before an individual's federal debt information may be referred to a private credit bureau.

— In 1984, Congress enacted the Cable Communications Policy Act to safeguard the confidentiality of interactive cable television subscriber records. The Act includes the highest court order standard ever enacted that must be met by law enforcement before subscriber records can be disclosed. The Act requires that cable subscription records may only be disclosed pursuant to a court order that shows by "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case." Further, the individual must have the opportunity to challenge the court order before the records are disclosed.[70]

— In 1986, the Electronic Communications Privacy Act (ECPA) was passed, amending the Wiretap Law to cover the interception of *non*-aural communications. Under the Act, law enforcement officials may not obtain information held by a data communications company, such as MCI, without a warrant that meets the probable cause standard. ECPA also overturns the Supreme Court's ruling in *Smith* v. *Maryland* that telephone toll records are not private. Under ECPA, law enforcement officials must show there is "reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry," before obtaining access to transactional data such as telephone toll records. ECPA represents a recognition of the need to protect information regardless of the technological advances that have shaped its use.

— The Video Privacy Protection Act of 1988, passed at the end of the 100th Congress, includes a strong court order standard modeled on the Cable Act. Videocassette rental records, like cable subscriber records, can reveal information about individual preferences and political beliefs. Congress has been quick to create strong protections in such areas where First and Fourth Amendment concerns intersect.[71]

These recent laws reflect Congress' willingness to fashion strict disclosure standards for sensitive information held by private institutions. Implicit in these new laws is a legislative recognition that

expectations of privacy can be created and enforced—a particularly crucial recognition in an age in which information practices continue to erode our constitutionally protected "reasonable" expectations.

IV. PROPOSALS FOR THE FUTURE

A. The Rewrite of the Privacy Act

There is a general consensus that the Privacy Act of 1974 is ineffective, obsolete, and needs to be rewritten.[72] Neither the absence of a vigorous privacy protection commission nor scattered, weak implementation by OMB can be blamed exclusively for the law's failure. At this stage, the emphasis should be on rewriting the Privacy Act. A privacy oversight agency, without strong, clear provisions to enforce, would continue to be a political tool in the hands of changing administrations.[73]

Only enforceable limits on what personal information can be collected and how it can be used can give individuals meaningful control over the information they divulge in exchange for receiving benefits and services from the government. The Act currently lacks such substantive limits.

In addition, much of the Act has been rendered obsolete by advances in information technology and the drive to adopt new technological capacities for data collection and consolidation. Recent statutes take into account more modern techniques of intrusion, but, on the whole, privacy legislation has not effectively erected barriers around information. Instead, the Privacy Act and the bulk of information privacy statutes aimed at information held by private institutions, require only that a series of procedural maneuvers be completed before an agency or institution can divulge records.

Due process safeguards are more than just good "data use manners," and may be genuinely protective in some instances, but more is needed rotect individuals. Notice and consent procedures are not g enough protection for personal information in the control of . overnment; *the government's collection and use of*

certain types of information, such as for tax, census, and public benefit purposes, should be limited, and even, in some cases, prohibited. Such limits are necessary to give individuals meaningful control over information about themselves; to grant people the right to control what the government (and others) may know about their lives.

The law should be redrafted to strengthen the Act's fundamental principles, giving individuals tangible control over information they disclose to government agencies either by law (i.e., for census and tax purposes) or as a condition of receiving government benefits or services. Government agencies should be authorized to collect only information that is necessary and relevant to their particular purpose. Agencies must inform individuals of the reasons why personal information is being collected and for what purposes it will be used. An individual must have the right to challenge a particular collection or use either through administrative or court action. The Privacy Act already includes an adequate procedure for agencies to follow before disclosing records pursuant to a law enforcement investigation.

In addition, the Act's "routine use" exemption must be revamped so that the law will work as intended. A clear and restrictive definition of routine use must be added to the statute clarifying that disclosure for a routine use must be *consistent* with the original purpose for which the information was initially collected. Individuals must have the right to challenge a proposed routine use on the grounds that it is not consistent with the purpose for which the information was originally collected. Routine use disclosures under this definition must be benign and not for the purpose of taking adverse action against an individual.

The Privacy Act needs a new remedy section that provides both liquidated damages and injunctive relief for any aggrieved individual. Currently, an indiviual may not sue under the Act unless he or she can prove willful and intentional misconduct by an agency official. Individuals must be able to collect damages for intangible harms caused by violations of the Act.

B. Information Privacy Policy Initiatives

For the future, privacy advocates must push for policy initiatives to protect medical, insurance, personnel, and retail records as well as personal information held by the government. The policy goal is the creation of federal statutory rights of information privacy, tailoring standards that incorporate a balance between the sensitivity of the information at stake and the institutional justification or need for the information— the more sensitive the information, the more compelling the need must be for its collection and the higher the standard must be for its disclosure to others.

The guiding principles in drafting legislation should be:

1) **Information collected for one purpose should not be used for a different purpose without the individual's consent.** Any unauthorized use of the information must give rise to an enforcement action by the harmed individual. The goal is to create legislatively mandated expectations of privacy in information.

2) **Policy should be developed with an eye towards new advances in information technology and telecommunications.** It may not be possible to anticipate every advance, but the law should be elastic enough to apply to information regardless of whether it is in electronic or manual form. In this way, the numbing cliché that technology is constantly outpacing the law may be overcome.

3) **Legal limits should be placed on the collection and use of sensitive information— the more sensitive the information, the more rigorous the disclosure standard.** Personal information, such as census data and certain medical records, should never be disclosed for any purpose, whereas less sensitive records might be available for legal proceedings. For sensitive information, law enforcement officials must demonstrate probable cause or reasonable suspicion

to believe a crime has been committed and that the information they seek relates to that crime. Individuals must receive notice before a court-ordered disclosure, and have an opportunity to challenge the disclosure.

4) **Individuals must be provided with easy access to their records, including access to computerized records, for the purpose of copying, correcting, or completing information in the records.** Computer technology should allow indiviuals on-line access to their records.[74] Legislation should mandate an access procedure, and require that information be kept accurate, complete, and up-to-date. Records that are no longer relevant for the purpose for which they were collected should be destroyed.

5) **Exemptions for non-disclosure should be clearly justified and narrowly tailored to suit the requestor's need.** Exemptions should explicitly define the intended scope of the allowable disclosure to avoid expansion or misinterpretation of the provision.

6) **Legislation should include enforcement mechanisms, such as injunctive relief, civil damages, criminal penalties, and reimbursement of attorney's fees and costs.** By putting teeth into information privacy legislation, individuals will be able to enforce the law and seek redress for violation of their privacy rights. Injunctive relief can prevent damage before it occurs, damages can compensate aggrieved individuals, and criminal penalties can punish those who violate the law. In addition, these individual enforcement mechanisms can be buttressed by institutional enforcement and oversight, such as by the promulgation of implementation guidelines, giving Privacy Act officers in each agency greater enforcement powers, and strengthening congressional oversight. Each of these enforcement mechanisms will deter unauthorized information gathering and exchange.

Momentum exists for building on recent successes to press for new information privacy initiatives. Work should continue towards the passage of laws that incorporate standards tailored to the sensitivity of the information involved.

V. CONCLUSION

Our right to privacy dwindles each year, giving way under the tremendous institutional pressure to collect and use information. The push for strong laws to protect information privacy is not a partisan issue. As stated in the 1980 Republican Party Platform:

> Government in recent years, particularly at the Federal level, has overwhelmed citizens with demands for personal information and has accumulated vast amounts of such data through the IRS, the Social Security Administration, the Bureau of the Census, and other agencies. Under certain limited circumstances, such information can serve legitimate societal interests, but there must be protection against abuse. . . We are alarmed by Washington's growing collection and dissemination of such data. There must be protection against its misuse and disclosure.

The momentum to protect personal information held by federal agencies, sparked by years of hearings, privacy abuses and culminating in the Watergate scandal, was maintained long enough for Congress to pass the Privacy Act of 1974. In addition, Congress has responded to the pressing need to protect personal information maintained by private institutions. Privacy advocates must continue to seize upon such targets of opportunity to heighten public awareness about the need for privacy legislation. Advances in information technology create legislative opportunities. Again, the Department of Health and Human Services is moving forward with a plan to link computers in 52,000 pharmacies nationwide to centralize, exchange, and audit information on Medicare beneficiaries. The FBI is proposing a massive expansion of its central computer system. These proposals all pose serious threats to individual privacy. Privacy advocates must inject their voices into the planning process to create a forum for debate on information and individual privacy.

Notes

1. *Olmstead* v. *United States*, 277 U.S. 438, 478 (1928) (J. Brandeis dissenting).

2. House Comm. on Government Operations, *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and the Congress*, H.R. Rep. 455, 98th Cong., 1st Sess. (1983).

3. L. Harris, *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (1983) (hereinafter Harris Survey). This Harris Survey documented that in 1983 forty-eight percent of the public described themselves as "very concerned" about technology and threats to personal privacy, double those in 1978. Sixty percent of the public believe the use of computers must be severely limited to safeguard privacy. A majority of the public takes the position that the release of personal information by government agencies to other agencies seriously invades personal privacy.

4. Harris Survey.

5. In 1987, Congressman Don Edwards (D-CA) convened a panel of privacy, criminal justice, and computer security experts to evaluate a set of FBI-developed changes to its information systems. The panel's report, submitted for consideration to the FBI's Advisory Policy Board (APB), appears to have had an impact on the decisionmaking process. Of the 246 proposals originally contemplated by the APB, only 81 were ultimately recommended for implementation. The panel is continuing to critique an FBI proposal to use the NCIC to track and surveil individuals suspected of certain crimes.

6. The proposed system involves the participation of 52,000 pharmacies across the nation in a computer network designed to process electronically the prescription drug bills of 32 million Medicare beneficiaries. The Health Care Financing Administration branch of HHS is currently seeking input on the implementation of the system, with a proposal for funding to be submitted in the fall of 1989. Privacy advocates plan to press for the incorporation of substantive privacy protections before the funding proposal is submitted.

7. Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, at 1 (1986) (hereinafter OTA Report).

8. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Prosser*, 39 N.Y.U. L. Rev. 962 (1964).

9. For purposes of this paper, the ability to control information about one's self is termed "information privacy," traditionally defined as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." A. Westin, *Privacy and Freedom*, at 39 (1967).

10. *NAACP* v. *Alabama*, 357 U.S. 449 (1958); *Stanley* v. *Georgia*, 394 U.S. 557 (1969).

11. *Mapp* v. *Ohio*, 367 U.S. 643 (1961).

12. *Griswold* v. *Connecticut*, 381 U.S. 479 (1965).

13. *Meyer* v. *Nebraska*, 262 U.S. 390 (1923).

14. *Boyd* v. *United States*, 116 U.S. 616 (1886); *Katz* v. *United States*, 389 U.S. 347 (1967).

15. Shattuck, *In the Shadow of 1984. National Identification Systems, Computer Matching, and Privacy in the United States*, 35 Hastings L.J. 991 (1984).

16. *Boyd* v. *United States*, 116 U.S. 616, 630 (1886).

17. Shortly after *Boyd*, came the publication of Warren and Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

18. *NAACP* v. *Alabama*, 357 U.S. 449 (1958).

19. *Katz* v. *United States*, 389 U.S. 347, 353 (1967).

20. In 1986 the Supreme Court, in *Bowers* v. *Hardwick*, 478 U.S. 186 (1986), *rehearing denied*, 478 U.S. 1039 (1986), upheld Georgia's sodomy statute, finding that one does not have a constitutional right to privately engage in consensual sexual conduct. In that case, Georgia charged a man with violating the state's criminal sodomy statute after "catching" him in the act in his own bedroom. The police entered the home to execute a warrant for a traffic violation.

21. 56 U.S.L.W. 4409 (U.S. May 16, 1988) (No. 86-684).

22. Uviller, "The Fourth Amendment: Does it Protect Your Garbage?", *The Nation*, October 10, 1988, at 303.

23. 425 U.S. 345 (1976).

24. A similar analysis was used to find that one does not have a reasonable expectation of privacy in telephone toll records, *Smith* v. *Maryland*, 442 U.S. 735 (1979).

25. Banks, in essence, perform a fiduciary/trustee function with regard to customer records. Thus, a customer may relinquish physical possession of his or her records, while still maintaining some element of control or ownership of the records.

26. *United States* v. *Miller* at 449-452, quoting *Burrows* v. *Superior Court*, 529 P. 2d 590 (1974)

27. 429 U.S. 589 (1977).

28. *Id.* at 605. In a recent case involving whether the FOIA applies to the release of criminal history records maintained by the FBI, Judge Starr of the District Court of Appeals noted in his dissent that if the FBI is required to release records from its name-indexed, computerized files, "the federal government is thereby transformed in one fell swoop into the clearinghouse for highly personal information, releasing records on any person, to any requester, for any purpose. . . . [T]his new-fangled regime will have a pernicious effect on personal privacy interests in conflict with Congress' express will." The Supreme Court agreed to hear the case, and briefs were submitted in June, 1988. *Reporter's Committee for Freedom of the Press* v. *Department of Justice*, 831 F.2d 1124 (D.C. Cir. 1987), *cert. granted*, 56 U.S.L.W. 3718 (U.S. April 18, 1988) (No. 87-1379)

29. *See* text at 21-22 *infra*.

30. *The Computer and Invasion of Privacy: Hearings Before the Special Subcomm on Invasion of Privacy of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966) (hereinafter 1966 House Privacy Hearings); *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92nd Cong., 1st Sess. (1971) (hereinafter 1971 Senate Privacy Hearings; and *Privacy: The Collection,*

Use and Computerization of Personal Data: Joint Hearings Before the Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 93rd Cong., 2d Sess. (1974).

31. 1966 House Privacy Hearings, at 2 (statement of Rep. Cornelius Gallagher (D-NJ)).

32. *Id.* at 6 (statement of Rep. Horton).

33. The House Special Committee on Invasion of Privacy released a report in 1968 "Privacy and the National Data Concept," recommending that plans for a data center be postponed until the confidentiality and security of centralized information could be assured.

34 1966 House Privacy Hearings, at 120-122 (testimony of Paul Baran, Rand Corp.)

35. H.R. Rep. No. 1416, 93rd Cong., 2d Sess. 3 (1974), *reprinted in*, Source Book, at 296. Also during this period, a number of books were published that signaled the decline of freedom in the new age of computerized data banks. See Miller, *The Assault on Privacy* (1971) and Westin and Baker, *Databanks in a Free Society. Computers, Recordkeeping, and Privacy* (1972).

36. U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973).

37. Privacy Act of 1974, 5 U.S.C. §552a (2)(a) (1974).

38. Cong. Rec. S. 6741 (May 1, 1974) (Introductory Remarks of Sen. Ervin on S 3418) *reprinted in* Senate Comm. on Government Operations and Subcomm. on Government Information and Individual Rights of the House Comm. on Government Operations, 94th Cong., 2d Sess., *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 5 (Joint Comm. Print 1976) (hereinafter Source Book).

39. *Id* at 30, *reprinted in*, Source Book, at 183. The Senate Committee report on the Privacy Act described the burgeoning use of the Social Security number as "one of the most serious manifestations of privacy concerns in the nation," clearing the way for a national data bank. *Id.* at 28, *reprinted in*, Source Book, at 181.

40. S. Rep. No. 1183, 93rd Cong., 2d Sess. 1 (1974), *reprinted in*, Source Book, at 154.

41. In a 1986 report, the congressional Office of Technology Assessment (OTA) found that federal agencies and departments held 3.5 billion records in the record systems as defined by the Privacy Act. Nearly half of those systems were computerized, with agencies reporting an increase in microcomputers from a few thousand in 1980 to 100,000 in 1985. OTA Report, at 12.

42. 5 U.S.C. § 552a (b)(3) (1974).

43. A 1980 notice of a proposed match published in the *Federal Register* stated that a match between the records of Office of Personnel Management (OPM) and the Veterans' Administration was for a "routine use": "An integral part of the reason these records are maintained is to protect the legitimate interests of the government, and therefore, such a disclosure is compatible with the purposes for maintaining these records."

44. Source Book, at 859-860.

45. *Computer Matching and Privacy Protection Act of 1986: Hearings on S. 2756 Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 99th Cong., 2d Sess. at 29 (Comm. Print 1986) (Ronald Plesser testifying on behalf of the American Bar Association).

46. Letter from Carl F. Goodman, General Counsel, Civil Service Commission, to Charles Ruff, Deputy Inspector General, Department of Health, Education and Welfare, (July 27, 1977), *reprinted in, Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. at 122-25 (Comm. Print 1982).

47. *Id.*

48. A 1986 Office of Technology Assessment (OTA) report found that matching has become an integral part of the operation of many government agencies. In 1984, agencies conducted 110 separate matching programs, totalling nearly 700 matches and involving 2 billion separate records. OTA Report.

49. 5 U.S.C. § 552a (1974).

50. Tax Reform Act of 1986, 26 U.S.C. § 6109 (e) (1986).

51. In contrast, all of the federal wiretap statutes provide for liquidated damages. *See* e.g., the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (1986).

52. The Privacy Protection Study Commission, *The Privacy Act of 1974: An Assessment*, (1977) (hereinafter Privacy Protection Commission Report).

53. Privacy Protection Commission Report, app. 4, at 113.

54. *Id.* at 120.

55. *Id.* at 21.

56. *Oversight of the Privacy Act of 1974: Hearings before a Subcomm. of the House Comm. on Government Operations*, 98th Cong., 1st Sess. 259 (1983) (statement of John Shattuck, ACLU) (hereinafter 1983 House Privacy Act Oversight Hearings). *See also*, House Comm. on Government Operations, *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and the Congress*, H.R. Rep. No. 455, 98th Cong., 1st Sess. (1983).

57. 1983 House Privacy Act Oversight Hearings, at 5 (opening Statement of Rep. English (D-OK)).

58. David Burnham, *The Rise of the Computer State* (1985).

59. *See* note 4 *supra*.

60. Deficit Reduction Act of 1984, 98-369, 98 Stat. 494 (1984).

61. 26 U.S.C. § 6109 (e) (1986).

62. The legislative history of the Privacy Act reveals Congress' previously deep concern about the expanded use of the Social Security number: "[O]nce the Social Security number is set as a universal identifier, each person would leave a trail of personal data behind him for all his life which could be immediately reassembled to confront him. . . . [W]e can be pinpointed wherever we are, we can be more easily manipulated, we can be more easily conditioned and we can be more easily coerced." Cong. Rec. (September 19, 1974) (statement of Sen. Goldwater), *reprinted in*, Source Book, at 760. In addition, government agencies are considering proposals for a national identification card to enforce the Immigration Reform Act, to distribute food stamps, and to process welfare applications.

63. 1971 Senate Privacy Hearings, pt. 1, at 9.

64. The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. 552a (1988).

65. § 15 U.S.C. § 1681 (1970).

66. 20 U.S.C. § 1232g (1974).

67. 12 U.S.C. § 3401 (1978).

68. 42 U.S.C. § 2000aa (1980).

69. 31 U.S.C. § 952 (1982).

70. Cable Communications Policy Act, 47 U.S.C. § 551 (1984).

71. The initiative for the Video Privacy Protection Act grew out of the unauthorized disclosure of the Bork family's video rental list to a reporter during Judge Robert Bork's confirmation hearings for the United States Supreme Court. At that time, many Senators expressed outrage at this intrusion into the Bork family's privacy, characterizing the disclosure as an "issue that goes to the deepest yearning of all Americans that we ...cherish our freedom...[and] we want to be left alone." *Nomination of Robert H. Bork to be Associate Justice of the Supreme Court of the United States: Hearings before the Senate Committee on the Judiciary*, 100th Cong., 1st Sess., 1374 (1987) (remarks of Sen. Patrick Leahy, D-VT).

72. In its 1986 report, OTA concluded that "federal use of new electronic technologies in processing personal information has eroded the protections" of the Privacy Act. OTA found that many information practices are not covered by the Act, and that there is scant oversight and inadequate remedies to ensure agency compliance. OTA Report at 4.

73. In 1977, the Privacy Protection Study Commission recommended that a privacy protection agency be established, but in conjunction with the passage of strong, enforceable information privacy laws. At that point, the Privacy Act should have been strengthened by legislative amendment, agency regulations, and strict congressional oversight.

74. Computer technology should be used to enhance privacy. For instance, computer audit trails can be used to inform citizens about how information about them is used, and may act as a deterrent to unauthorized access and unnecessary uses of personal information.

About This Series

This publication is one of eight papers that comprise the Benton Foundation Project on Communications & Information Policy Options. Papers may be ordered individually, or as a boxed set, by contacting the foundation at the address below.

Papers in this series include:

1 *The Role of Public Policy in the New Television Marketplace*
Jay G. Blumler
University of Leeds and University of Maryland

2 *Public Broadcasting*
Harry M. Shooshan III and Louise Arnheim
Shooshan & Jackson Inc.

3 *Charging for Spectrum Use*
Henry Geller and Donna Lampert
Washington Center for Public Policy Research
Duke University

4 *A Federal Right of Information Privacy: The Need for Reform*
Jerry Berman and Janlori Goldman
American Civil Liberties Union

5 *Watching the Watchers: The Coordination of Federal Privacy Policy*
George Trubow
The John Marshall Law School

6 *Strengthening Federal Information Policy Opportunities and Realities at OMB*
Gary Bass and David Plocher
OMB Watch

7 *A Presidential Initiative on Information Policy*
John Shattuck and Muriel Morisey Spence
Harvard University

8 *The Federal Structure for Telecommunications Policy*
Henry Geller
Washington Center for Public Policy Research
Duke University

Individual copies are $6 50 each, including postage and handling. The boxed set of eight papers is available for $33.00, including postage and handling. A bulk discount of 10% is available for orders of 10 or more copies of the same paper Checks or money orders should be made payable to the Benton Foundation and mailed to.

Policy Options Project
Benton Foundation
1776 K Street, N.W
Washington, D.C 20006

BENTON FOUNDATION

1776 K Street, N.W.
Washington, D.C. 20006